AK IT-Security 1

Current research
Identity management

Thomas Lenz
Graz, 12.11.2014
Overview

» Identity Management
  » Retrospection
  » Single Sign-On session security
  » Dynamic attribute generation
  » Trust management
Identity Management in Austria

- Identity data stored in user-domain
- Usually stored on a secure token (e.g., smart card)
- Explicit user consent
- e.g., Citizen Card, nPA

Ref: Palfrey and Gasser, 2007
MOA-ID

» High secure authentication
  » Based on the citizen card (smart card or mobile phone signature)

» No first contact respectively registration needed
  » Unique identification is based on the identity link

» Simple integration into online applications
  » Authentication data are transferred to the online application
MOA-ID 2.x Architecture
New requirements

» Single Sign-On (SSO)
  » Secure a SSO session
  » Terminate SSO sessions
  » Timeout synchronization and keep-alive messaging
  » SSO session transfer

» Dynamic attribute generation

» Trust management between participants
SSO Session Security

» HTTP cookies are the commonly used method for SSO session identification
  » Are HTTP-cookie sufficient?

» Additional provisions required?
  » Holder-of-Key
  » Unique-Session Binding
  » Second channel for SSO session authentication
  » JavaScript or browser based solution
Holder-of-Key

User  Browser  Online-Application  MOA-ID 2.x IDP

- Generate keypair
- AuthRequest
- TLS + client cert. authentication
- Authentication
- AuthResponse
- TLS + client cert. auth.
- Match cert. from TLS channel with cert. from assertion
- Extract certificate
- Add certificate
Unique-Session Binding

» Communication over SSL/TLS channel

» Unique-Session binding use the SSL/TLS resume-session functionality to reuse an old SSL/TLS session

» Is this feature suitable to improve SSO session security?
Modern authentication processes use more channels to perform a secure authentication.

Such a second channel can also be used for SSO session authentication.
Terminate SSO sessions

- There are many single http sessions
- How to terminate every single session or is this feature required?
- Single Logout (SLO) contrary process to SSO
  - Logout at all services a user is currently logged in
  - Important security feature
- Actually open problems
  - Not supported by all protocols
  - Who starts a SLO process?
  - When a SLO process is started?
  - Global logout or partial logout?
http Session Synchronization

» Heterogeneous service model
» Every single http session between user and service provider could have a different timeout
» Trade-off between security and usability
» Are there solutions to synchronize http session timeouts?
SSO session transfer

» Identity Provider point of view

» Identity Federation

» Share SSO identity information between different identity providers

» Required trust management between IDPs
SSO session transfer

» Users point of view
  » A SSO session is bound to one browser and device
  » User has different devices with different application
  » As example: Transfer a active session from PC to smartphone without re-authentication.
Dynamic attribute generation

» Actually, identity data (identity link) is stored in user-domain on a secure token

» Identity link includes all personal information

» Identification and authentication is performed by using this secure token.
  » Identification: Identity link
  » Authentication: Secure token and PIN/Password

» How to decouple identification and authentication?
Online identity link

» Dynamic generation after authentication
» Could be done by using an identity management service
» Include bPK/wbPK instead of source PIN
» Only include attributes which are actually required
» How couple identification data with authentication information?
Electronic mandates

» Electronic mandates include
  » Unique identifies (source PIN)
  » Scope of the power of representation

» Actually selected during identification and authentication process

» Make troubles in case of SSO
  » Scope of the power has to be mapped
Trust management

“Trust is the characteristic whereby one entity is willing to rely upon a second entity to execute a set of actions and/or to make a set of assertions about a set of principals and/or digital identities. In the general sense, trust derives from some relationship (typically a business or organizational relationship) between the entities” [Goodner and Nadalin]

» Indirect Trust rely on claims asserted by an intermediary or a common trusted third party

» Direct Trust

» One party fully trusts the other party without any intermediaries or another trusted third party
Direct Trust

- Use previously exchanged information in most cases (Whitelist with certificates, ...)
- Limitation in case of a dynamic heterogeneous service model

How to create trust without previously exchanged information?
Thank you for your attention

Thomas Lenz –
thomas.lenz@egiz.gv.at
www.egiz.gv.at

EGIZ
E-Government Innovationszentrum